



Department of Economic Security
Information Technology Standards

Title: 1-38-0015 DES Internet Use Policy

Subject: Implementation and Support of Internet Services used by DES.

Effective Date:

07/28/2000

Revision:

1.3

1. Summary of Policy Changes

- 1.1. 10/17/01 - Annual review and adjustments to recognize 1-38-0029, the DES Information Technology (IT) and Office Equipment and Resources Acceptable Use Policy.
- 1.2. 05/02/03 – Addition of a Reference to A.R.S. §, 38-448 State employees; access to internet pornography prohibited; cause for dismissal; definitions.
- 1.3. 05/11/04 – Added text about Internet Monitoring Policy and ISA Logs in 6.4.

2. Purpose

Information technology (IT) resources provided by the Department of Economic Security, including the Internet, are intended to support the agency's programs in achieving their missions and goals, and to improve state government in general. DES IT resources are intended to facilitate day to day operations, including collaboration and information exchange within and between state agencies, branches of government, and others. They are also intended to expedite public access to information.

DES intends to provide, exchange, and access information via the Internet, so it is necessary to support such services by establishing policies and procedures to ensure security of data resources and productive use of those resources.

This policy establishes the rules by which DES and its various subdivisions will administer Internet related systems.

This policy defines acceptable and unacceptable uses of the Internet by DES employees and provides guidelines to appropriately use electronic communication facilities provided by DES.

It is intended to:

- 2.1. Ensure the security and integrity of DES computing systems;
- 2.2. Maintain the legal confidentiality of employee and client records and information;
- 2.3. Ensure the proper use of DES systems by authorized users;
- 2.4. Ensure information provided by DES via the Internet/Intranet/Extranet is accurate, legal, and non-discriminatory;
- 2.5. Define responsibilities for building and maintaining The DES Internet related infrastructure.

3. Scope

This policy applies to all DES divisions and programs, boards and commissions.

This policy applies to all Internet/Intranet/Extranet systems used within DES.

This policy applies to all authorized users of DES systems, defined as DES employees, contractors, temporary staff members, or any other person with management approval to access DES computing systems.

4. Responsibilities

- 4.1. The DES Director, Deputy Directors, Associate Director, and Assistant Directors are responsible for enforcing this policy, and for investigating suspected non-compliance.
- 4.2. The DES Office of Communications is responsible for designing and maintaining the DES “Home Page” and for establishing standards for the appearance and acceptable content of subsidiary DES web pages.
- 4.3. The Division of Technology Services is responsible for implementing this policy, monitoring DES compliance, and for establishing standards for programming languages and techniques used for Internet publishing.
- 4.4. DES Internet Users are responsible for following all DES Internet policies, procedures, and standards.

5. Definitions and Abbreviations

5.1. Definitions

- 5.1.1. **Download** – As used in this policy, downloading refers to saving information, in a digital format, such as to a disk or hard drive.
- 5.1.2. **E-mail** – Electronic mail is the transmission of messages over a network. Electronic mail requires a messaging system that provides store and forward capabilities as well as a user interface that provides send and receive functions.
- 5.1.3. **Internet** – A huge computer network comprised of many computer networks located worldwide. Distinguished from the World Wide Web which is the body of information accessed via the Internet.
- 5.1.4. **Internet User** – As used in this policy, Internet user refers to an agency employee, contract employee or other agency authorized person who accesses the Internet through the use of state/agency owned/controlled computer equipment.
- 5.1.5. **Network** – Two or more computers connected to share resources. Those resources may include information or peripheral resources such as a printer. A network may be a LAN (Local Area Network) or a WAN (Wide Area Network).
- 5.1.6. **Public Domain** - Property rights that are held by the public at large. Public domain material exists without copyright protection.
- 5.1.7. **Virus** – As used in this policy, virus means software used to infect a computer. Once virus code is written it is buried within an existing program. When the program is executed the virus code is activated.

5.2. Abbreviations and Acronyms

- 5.2.1. **ARS** - Arizona Revised Statutes
- 5.2.2. **DES** – Department of Economic Security
- 5.2.3. **DTS** – Division of Technology Services
- 5.2.4. **ET** – DES Executive Team
- 5.2.5. **GITA** - Government Information Technology Agency
- 5.2.6. **IT** – Information Technology
- 5.2.7. **ITSP** - Information Technology Strategic Plan
- 5.2.8. **CIO** – Chief Information Officer
- 5.2.9. **ISA Logs** – Internet Usage Logs

6. POLICY

6.1. General Internet Policy Statements:

- 6.1.1. DES and its Internet users shall comply with all applicable federal and state laws, regulations, agency policies, procedures and guidelines.
- 6.1.2. Internet use is a privilege, not a right. Violation of this policy may result in revocation of the privilege and/or disciplinary action.
- 6.1.3. Each DES division or administration may provide specific documentation of allowable Internet activity and proper use within its respective program(s), not to exceed the restrictions stated in this document.
- 6.1.4. DES systems and all information stored on them are the property of DES.
- 6.1.5. All connections of the DES network to the Internet must provide a measure of protection against inappropriate access and network address conflict. This includes dial-up access, peer-networking or any other type of connection that may become available. The firewall will be configured to enforce the policies defined in this document.
- 6.1.6. Information passed into the DES network from the Internet must be checked for viruses. In addition, each DES personal computer with access to the Internet through an alternative Internet Service Provider must have current virus checking software installed and operating.
- 6.1.7. Users of the DES Internet Center for Internet or Intranet access will share in the costs on a prorated basis. Users of external Internet Service Providers will be responsible for the direct costs generated by their respective contracts and/or use.
- 6.1.8. Each division or administration is responsible for the costs of any software or hardware necessary to enable their users to connect to the Internet. All software and hardware must be purchased through the standard DES procurement procedures normally used for these products.
- 6.1.9. Internet access is an information technology/computer service and is the property of DES and the State of Arizona.
- 6.1.10. DES reserves the right to monitor Internet use and/or examine electronic mail by any user at any time. The DES Director (or designee) may determine appropriate use and may deny, revoke, suspend or close any user account at any time, based upon a determination of inappropriate use, as defined in 1-38-0029, the DES Acceptable Use Policy. Users should be aware that monitoring Internet use, including sites visited, can be accomplished without user consent, and may occur without prior notice.
- 6.1.11. All communications and information accessible via the Internet should be assumed to be copyrighted and private property. DES Internet users shall honor copyright laws including those protecting software and intellectual property.
 - 6.1.11.1. Duplicating, transmitting, or using software not in compliance with software license agreements is considered copyright infringement.

General Internet Policy Statements (continued):

- 6.1.11.2. Users shall not make copies of software or literature without authorization and the full legal right to do so.
- 6.1.11.3. Unauthorized use of copyrighted materials or another person's original writings is considered copyright infringement.
- 6.1.11.4. Internet users shall not transmit copyrighted materials, belonging to others, over the Internet without permission.
- 6.1.11.5. Users may download copyrighted material from the Internet, but its use must conform with the restrictions posted by the author or current copyright law.
- 6.1.11.6. Copyrighted information used on Web sites must be clearly identified as such.
- 6.1.12. The same policy for retention of records as set forth in DES 1-01-13, the DES E-Mail Use Policy shall apply to all records obtained or received via the Internet. DES employees who transmit or receive material via the Internet shall determine whether to preserve or delete the material and communications consistent with the records retention schedule and DES records retention policy.
 - 6.1.12.1. DES employees with questions regarding records retention should contact their supervisor and ARS § 41-1347, 41-1350, and 39-121.01(B).
 - 6.1.12.2. Routine E-mail and communications (similar to oral conversation and voice mail, defined as expeditious communication on routine matters such as scheduling meetings and conference calls) may be deleted after the required action is taken.
- 6.1.13. DTS is responsible for the support of the DES Internet Center.

6.2. Web Site Administration Policy Statements:

- 6.2.1. DES will have only one Home Page, which will be maintained and accessed at the domain name (URL) www.de.state.az.us
- 6.2.2. The appearance of the DES Home Page will be designed by the DES Office of Communications.
- 6.2.3. The Division of Technology Services will establish standards for programming languages and techniques used for Internet publishing.
- 6.2.4. The DES Home Page will provide links to other DES divisions, administrations or program-specific web pages.
- 6.2.5. Administrations may publish web pages with the approval of the respective Assistant Directors and in compliance with this policy and other DES Office of Communications and Division of Technology Services rules.
- 6.2.6. DES web page content shall be consistent with the mission of DES and shall adhere to the security and confidentiality policies and statutes supported by DES and the State of Arizona.
- 6.2.7. Web sites referenced within DES maintained web pages must relate to the mission of DES.
- 6.2.8. This policy applies to DES web content maintained on external Internet service providers' servers.

Web Site Administration Policy Statements (continued):

- 6.2.9. The creation and maintenance of web pages (i.e. authoring HTML) should be managed the same way as other software development projects. This includes internal resources, DTS Systems and Programming or third party resources as appropriate for the division or program.
- 6.2.10. The Division of Technology Services standards for programming languages and techniques for Internet publishing, and any other related DES Office of Communications and/or Division of Technology Services rules, must be followed regardless of the resource(s) used to create and maintain web pages.
- 6.2.11. The DES infrastructure is the preferred method of connecting to the Internet. If this is not feasible, alternative Internet Service Providers may be used to provide access to DES authorized users for the Internet. Connections to an alternative Internet Service Provider must include a software and/or hardware solution that isolates the DES computer network(s) and prevents access to inappropriate areas. Any connection to an external Internet Service Provider must be reviewed by DTS and approved by the respective division's Assistant Director.
- 6.2.12. Data security personnel will maintain and audit security mechanisms. Authorized users are specifically prohibited from testing, hacking, or probing security mechanisms at either DES or other Internet sites.
- 6.2.13. In the event that the protection of DES information is suspect and unauthorized disclosure is possible, corrective action must be immediately initiated by the respective division or program security representative, the Office of Data Security and Internet Center personnel.

6.3. Internet User Policy Statements:

- 6.3.1. The Internet is provided to DES employees to enhance performance of their duties.
- 6.3.2. DES employees' use of the Internet should be managed by rules of conduct as defined in 1-38-0029, the DES Information Technology (IT) and Office Equipment and Resources Acceptable Use Policy.
- 6.3.3. The truth or accuracy of any information obtained from the Internet should be considered potentially suspect unless validated.
- 6.3.4. A signed consent form will be required from all DES Internet users. Anyone with Internet access at DES must acknowledge and consent to the DES possession of, and access to, all network and information systems activity. The DES consent form is incorporated into this policy as **Attachment A**.
- 6.3.5. Authorized users are specifically prohibited from testing or probing security mechanisms at DES or other Internet sites.
- 6.3.6. User Training:
 - 6.3.6.1. The Division of Employee Services and Support, Organization and Management Development, shall develop a training course and related support for all DES Internet users. DES Internet training will not be performed at a division or program level.
 - 6.3.6.2. Each division or program is responsible for funding appropriate training and support on approved Internet services for its authorized users.

Internet User Policy Statements (continued):

- 6.3.6.3. New employees will be trained on proper use of the Internet at DES before they are authorized to use the Internet.
- 6.3.6.4. Current employees will be retrained on proper use of the Internet at DES on a regular basis, in accordance with DES training standards.
- 6.3.6.5. For purposes of this section, “employees” means DES employees, contractors, temporary staff members, or any other person with management approval to access DES computing systems.
- 6.3.7. Users must have completed the data security awareness training before access is granted.
- 6.3.8. Downloading information from the Internet is permitted only when it meets the restrictions of the DES Director or the Director’s information technology designee.
- 6.3.9. All DES employees with access to the Internet shall acknowledge and consent that all network and information systems activity is the property of DES and the State of Arizona, and therefore should not consider any Internet activity to be private.
- 6.3.10. Authorized users must follow all established business practices, and may not obligate DES in the selling or purchasing of any product or service. The terms and conditions specified in the license agreements which accompany “shareware” are specifically included in this requirement. Perpetual “evaluation” of a software product or repeated downloading of new “evaluation” copies of the software is prohibited. Use of such products to conduct normal day-to-day agency service, thus making DES *DE facto* dependent upon the products, prior to purchase of the products, is prohibited. Authorized users will adhere to all laws pertaining to copyrighted, trademarked or patented materials.
- 6.3.11. Without prior authorization from their Program Administrators, authorized users may not use DES systems to post information, opinions or comments to Internet discussion groups and other such forums, which reflect the official position of DES.
- 6.3.12. Communications on DES systems, including those connected to the Internet, must comply with the DES Communications Policy, and may not contain content that a reasonable person would consider to be defamatory, offensive, harassing, disruptive or derogatory of any person, entity or DES.

6.4. Internet Monitoring Policy Statements:

- 6.4.1. ISA logs are Internet usage logs which IP addresses access which web sites. They create 15GB of data each month. The DSA unit has been using these to search for inappropriate web usage by DES employees. A 12 month retention period is recommended.

7. Implications

All DES divisions and programs will comply with this policy.

This policy states each DES personal computer with access to the Internet through an alternative Internet Service Provider must have current virus checking software installed and operating. Some DES divisions may need to invest in appropriate software and infrastructure to keep the software current.

8. Implementation Strategy

All DES divisions and programs will implement this policy as soon as is possible, pending the availability of funding.

The Division of Employee Services and Support, Organization and Management Development, shall develop a training course for all DES Internet users. DES Internet training will not be performed at a division or program level.

9. References

9.1. Developmental References

9.1.1. DES 1-01-13.A	Electronic Mail Policy
9.1.2. A.R.S. §, 38-448	State employees; access to internet pornography prohibited; cause for dismissal; definitions
9.1.3. A.R.S. §, 39-121.01(B)	Copies, Printouts or Photographs of Public Records
9.1.4. A.R.S. §, 41-1347	Preservation of Public Records
9.1.5. A.R.S. §, 41-1350	Definition of Records
9.1.6. A.R.S. §, 41-3501	Definitions
9.1.7. A.R.S. § 41-3504	Powers and Duties of the Agency
9.1.8. ARS 13-2316	(Computer Fraud)
9.1.9. ARS 41-712	(Article 2 Automation Functions)
9.1.10. ARS 41-770	(Personnel Actions)
9.1.11. Public Law 93-589	(Privacy Act of 1974)
9.1.12. Public Law 100-235	(Computer Security Act of 1987)
9.1.13. Public Law 94-553	(U.S. Copyright Law)
9.1.14. 18 USC 1030	(Computer Fraud and Abuse Act of 1986)
9.1.15. 18 USC 2252	(Child Pornography)

9.2. Replaced References

9.2.1. None

10. Attachments

10.1. Attachment A - DES Internet Use Policy Consent Form

11. Associated GITA IT Standards or Policies

11.1. None

12. Review Date

12.1. This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.

Attachment A - DES Internet Use Policy Consent Form

This form's purpose and language was integrated into the J-129, DES User Affirmation Statement, which every DES employee signs.

DES Internet Use Policy Consent Form

I, _____, have read and understand the Arizona Department of Economic Security Internet Use Policy. I agree to comply with all terms and conditions of this policy.

I understand and agree that all network and information systems activity, conducted with state/agency resources, is the property of the Arizona Department of Economic Security and the State of Arizona.

I understand that the Arizona Department of Economic Security reserves the right to monitor and log all network activity, including electronic mail, with or without notice. I have no expectation of privacy in the use of these resources.

Signed: _____

Date: _____

LIABILITY

The Arizona Department of Economic Security makes no warranties of any kind, whether express or implied, for the use of the Internet or electronic information resources. Additionally, the Arizona Department of Economic Security is not responsible for any damages; whatsoever, that employees may suffer arising from or related to use of the Internet or electronic information resources.

DES Form Number